FILED
IN OPEN COURT
JAN 23 2020
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA v. ALEKSEI YURIEVICH BURKOV, *Defendant*.	Criminal No. 1:15-CR-245 Hon. T.S. Ellis III

STATEMENT OF FACTS

The United States and the defendant, ALEKSEI YURIEVICH BURKOV ("BURKOV"), agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence.

Count 2 – Access Device Fraud Committed Through the "CardPlanet" Website

1. From on or about October 23, 2011, through at least August 2013, BURKOV, knowingly and with intent to defraud, did traffic in and use one or more unauthorized access devices, to wit, payment card account numbers and card verification values, during a one-year period, to wit, from January 1, 2012, through December 31, 2012, and by such conduct did obtain things of value aggregating over $1,000, said trafficking affecting interstate and foreign commerce, in that the trafficking occurred via the Internet, and between computers located inside the Commonwealth of Virginia, and computers located outside of the Commonwealth of Virginia. Said trafficking also occurred outside the territorial jurisdiction of the United States and involved access devices issued, owned, managed, or controlled by U.S. financial institutions within the meaning of Title 18, U.S. Code, Section 1029(h).

2. From on or about October 23, 2011, through at least August 2013, BURKOV controlled and operated Cardplanet LLC and Cardplanet.cc ("Cardplanet"), which did business through the website www.Cardplanet.cc (the "Cardplanet Website"). The Cardplanet Website, which contained the user interface for customers who bought stolen payment card data, was hosted on a server located outside the United States. Cardplanet sold stolen payment card data for virtually all major U.S. payment cards, including cards under the "Company-1" brand and issued by "Bank-1." At all relevant times, "Company-1" was a major U.S. credit card company with data centers for processing payment card transactions located outside of the Commonwealth of Virginia, and "Bank-1" was a major U.S. bank that issued credit cards and had its corporate headquarters in McLean, Virginia, in the Eastern District of Virginia.

3. As a part of the fraudulent scheme, BURKOV offered a fee-based service "checker" on the Cardplanet Website that enabled customers to instantly validate stolen payment card numbers that the customer purchased. BURKOV also allowed Cardplanet's customers to search for stolen payment card information by state in which the victim lived. The purpose of this feature was to assist Cardplanet's customers in evading the fraud protections of U.S. payment card issuers by letting customers purchase stolen payment card data that belonged to victims in the area in which they intended to make fraudulent purchases.

4. As part of the fraudulent scheme, in order to maintain a constant supply of stolen credit and debit card data that could be sold on the Cardplanet Website, BURKOV solicited stolen payment card data from other cybercriminals, knowing that this data would be obtained via computer hacking. In particular, BURKOV cultivated relationships with fellow cybercriminals through his membership in cybercrime forums, including "Direct Connection," as explained below. Through these relationships and through advertisements placed on cybercrime forums

including Direct Connection, BURKOV was able to maintain a steady supply of stolen credit and debit card numbers which he then sold and offered for sale on the Cardplanet Website.

5. Through the Cardplanet Website, BURKOV offered for sale stolen payment card data from more than 150,000 compromised payment cards – including cards branded in the names of the largest credit card companies in the United States – knowing that such stolen data would be used to create counterfeit cards in order to make fraudulent purchases. The compromised cards sold on the Cardplanet Website included at least tens of thousands of cards which had been issued by over 10 U.S. institutions to cardholders in the United States, some of whom were residents of the Eastern District of Virginia. Many of the compromised cards had been issued by Bank-1.

6. As a further part of the fraudulent scheme, BURKOV's customers who purchased stolen payment card data on the Cardplanet Website encoded the data on counterfeit cards embossed with the corresponding payment card company's logo, without the payment card company's knowledge or consent. BURKOV's customers then used the counterfeit payment cards to purchase goods and services from merchants throughout the United States and elsewhere, including merchants located in the Eastern District of Virginia. A portion of the fraudulent purchases were made in person, by presenting the counterfeit payment card to the merchant. Other purchases were made over the Internet, without the fraudulent card being present. For example,

a. On or about February 3, 2012, one of BURKOV's customers engaged in a financial transaction at a fast food restaurant in Richmond, Virginia, in the Eastern District of Virginia, using a counterfeit Company-1 small business charge card encoded with stolen card data sold on the Cardplanet Website.

b. On or about March 15, 2013, one of BURKOV's customers engaged in a financial transaction at a convenience store in Fredericksburg, Virginia, in the Eastern District of Virginia, using another counterfeit Company-1 credit card encoded with stolen card data sold on the Cardplanet Website.

7. Stolen payment card data that BURKOV sold on the Cardplanet Website was used to commit over $20 million of fraudulent transactions.

Count 5 -- The "Direct Connection" Cybercrime Forum

8. From at least on or about February 21, 2009, through on or about December 13, 2015, BURKOV, did knowingly combine, conspire, confederate, and agree, with other persons known and unknown, to commit a variety of offenses against the United States, including:

a. To knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, knowing that the means of identification belonged to another actual person, with the intent to commit, and to aid and abet, and in connection with, any unlawful activity that constitutes a violation of Federal law, and that constitutes a felony under any applicable State or local law, where the production, transfer, possession, and use of said means of identification is in and affects interstate and foreign commerce, including the transfer of a document by electronic means, in violation of Title 18, U.S. Code, Section 1028(a)(7);

b. To traffic in and use one and more unauthorized access devices during a one-year period, and by such conduct obtain things of value aggregating $1,000 and more during that period, said use in violation of Title 18, U.S. Code, Section 1029(a)(2);

c. To knowingly and with intent to defraud, access a protected computer without authorization and by means of such conduct further the intended fraud and obtain something of value, specifically personal identifying information of others, in violation of Title 18, U.S. Code, Section 1030(a)(4);

d. To devise and intend to devise schemes and artifices to defraud, and for obtaining money and property, such schemes affecting financial institutions, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, including payment card-related information was transmitted over the Internet from merchant point-of-sale terminals in the Eastern District of Virginia to computers outside the Commonwealth of Virginia, in violation of Title 18, U.S. Code, Section 1343.

e. To conduct or attempt to conduct financial transactions which in fact involved the proceeds of specified unlawful activity within the meaning of 18 U.S.C. § 1956(c)(7), knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole or in part to

conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity, in violation of Title 18 U.S. Code, Section 1956(a)(1)(B).

9. In particular, BURKOV and his co-conspirators, some of whom operated from within the United States, created an online forum, which they called "Direct Connection." The purpose of the Direct Connection was to allow elite cybercriminals to meet in a secure location where they would have access to other elite and trusted co-conspirators and where they could plan and assist in cybercrimes, including the advertisement, purchase, and sale of stolen goods and illegal services. The stolen goods advertised on Direct Connection included stolen payment card data, stolen personal identifying information, and malware. The illegal services advertised on Direct Connection included money laundering services and access to networks of compromised computers.

10. It was further part of the conspiracy that BURKOV and his co-conspirators monitored and controlled access to Direct Connection so as to avoid infiltration from law enforcement and to ensure that Direct Connection members would honor the criminal agreements they made with one another. In order to join Direct Connection, three Direction Connection members had to "vouch" for an applicant, stating the applicant's history of committing cybercrime and reputation for cybercrime and dealing fairly with co-conspirators. In addition to having trusted members verify an applicant's membership through other cybercrime forums, the vouching members were required to commit to pay an amount of money, usually approximately $5,000 (normally split between the three "vouchers"), as insurance in case the applicant failed to make full payment while conducting criminal business on Direct Connection. For instance, in vouching for an applicant, one Direct Connection member posted, "I confirm financial liability of $1667. I've known this person for about 3 years. We used to work on a project with honest drops,"

referring to money laundering schemes in which the money mule is complicit. He continued, "[d]uring our cooperation [the applicant] proved to be a responsible, honest and a reasonable [sic]." A Direct Connection Member wrote of a different applicant, "I'm for him. He's a good drops manager," referring to a money launderer, "and a reasonable guy." Once an applicant had the requisite sponsors, all Direct Connection members were able to vote on whether to accept the applicant. Direct Connection members also monitored possible arrests of its members and removed the access of arrested members in order to prevent law enforcement from using cooperating forum members to infiltrate Direct Connection.

11. It was further part of the conspiracy that BURKOV and his co-conspirators organized Direct Connection into numerous sections where members can post comments on different topics. These sections, known as "forums," were labeled as follows (translated from Russian):

- News
- Stuff Carding-Drops for Stuff, Online Shopping
- Buying and Selling Cards, Visa, MasterCard, and Amex, Looking up SSN/DOB and other card holder information.
- Real Carding, Documents, Real Plastic, Equipment, Dumps (cashing /sales)
- Banking, Drops, account cashing, bank transfers
- Information Security, programing, intrusion, databases, botnets, Trojans, scripts and exploits.

As indicated by their titles, these forums covered such topics as credit card fraud, money laundering, malware, hacking, and shipping goods. In particular, "carding" refers to buying and selling stolen payment card information; "looking up by SSN/DOB and other card holder information," refers to services that allow cybercriminals to search for personal identifying information of particular victims; "Dumps" refers to stolen payment card information; "botnets"

refers to networks of compromised computers; "Drops" and "bank transfers" refer to money laundering services; and "trojans" and "exploits" are tools that can be used to gain unauthorized access to computers. Direct Connection members could create "threads" to each forum to discuss a designated topic by posting comments to that threat. Examples of some of the posts on Direct Connection include members soliciting or requesting to purchase stolen credit card data, members advertising data stolen from hacking, members selling malware to be used in computer intrusions, and members offering to launder the proceeds of cybercrime. For example,

a. On or about May 22, 2015, under the forum, "Banking. Drops. Accounts" and the thread "Banks. Accounts. Cash-out of bank transactions. How to work with drops. Merchants," a Direct Connection member posted: "Looking for continuous deposits on US prepaids. Quick cash-out on a POS with a daily limit."

b. On or about August 8, 2011, under the forum "Cards to sell and to buy," a Direct Connection member posted, "We're selling US CC with a known available balance. 100% validity. It's possible to pick by the state. Prices: $5 for a CC + $0.5 for every 1K on the balance (that is 1-2K available balance = $5.5, 2-3K = $6, 3-4K = $6,5 etc)," and provided his email address.

c. On or about May 27, 2010, under the Forum "Real plastic. Equipment, dumps (cash-out, sale). Documents and scans," a Direct Connection member posted: "Looking for people to withdraw the entire balance from US D+P. Balances start from 50K. Please PM me contacts and your interest rate." "US D+P" refers to stolen U.S. debit cards ("dumps") for which the theft has the corresponding pin number. The purpose of this post was to solicit assistance with stealing money from compromised U.S. debit card accounts.

d. On or about June 20, 2010, under the forum "Banks. Accounts. Cash-out of bank transactions. How to work with drops. Merchants," a Direct Connection member provided advice on how to launder money from U.S. banks, posting: "You can open an account online almost in every bank in the US, that's correct. The problem is that banks check addresses in public records and can ask you to come to their branch to confirm your personality."

e. On or about, November 3, 2015, under the forum, "Spam. Downloads and traffic. Hosting, domains and servers," and the thread, "Sales and purchase of downloads and traffic," a Direct Connection member posted: "I need US

and EU loads for a quiet and compatible software. I'm ready to align with almost anything except lockers, fake AV and other aggressive software. If you load a formgrabber, clicker, socks bot, or suchlike, please PM and we can agree on terms." This post offered web-hosting services to be used for computer hacking schemes.

f. On or about November 20, 2015, a Direct Connection member posted an advertisement indicating he wished to sell a database containing the names and dates of birth of over 191 million Americans. This database contains the personal information of American citizens, including some residing in the Eastern District of Virginia.

12. "PMs," as used above, refers to the "Private Message" feature of Direct Connection that enabled members to speak directly over the Direct Connection platform. As intended by BURKOV, members who wished to engage in criminal schemes together would often respond to a public post with a private message. Private messages often led to members exchanging contact information and continuing to work together towards Direct Connection's criminal aims. For instance, Direct Connection members sent each other the following private messages over Direct Connection:

a. On or about November 21, 2012, a Direct Connection member private messaged another member asking, "Regarding logs, I have some from 2011 and 2012, I can try and find about 200 Gb. How much do you pay and how much do you want to take? What else do I need for the account except the login and password?" This message concerned selling stolen login credentials.

b. On or about December 15, 2012, a Direct Connection member private messaged another member asking, "Hi, I'm writing regarding drops in the US. How can I contact you?" This message concerned laundering stolen money in the United States.

c. On or about July 13, 2013, a Direct Connection member private messaged another member asking "Hi. What kinds of goods are available and what is the approximate volume? I'm not a professional buyer, but I'm interested in buying in the US." This message concerned the sale of stolen U.S. payment card data.

d. On or about February 17, 2014, a Direct Connection member private messaged another member asking, "Hi, I have a lot of logs and I'm interested in work on an ongoing basis. Write if you need anything

specific." The message concerned working together to extract login credentials to financial accounts from data stolen via computer hacking and to use them to steal money from those accounts.

e. On or about May 7, 2010, a Direct Connection member private messaged another member in response to a post about withdrawing money from compromised U.S. debit card accounts, stating "Hello, I have an interesting offer for your question. If you have a good volume of D+P with a decent balance, I can deposit a good volume… Let's connect in Jabber, I'll tell you all the details! Different schemes!"

f. On or about October 10, 2011, a Direct Connection member private messaged another member, providing information about a bank account at a major bank in Hyattsville, Maryland, that included the account number and wire routing number. This message concerned making unlawful transactions from that account.

g. On or about November 14, 2011, a Direct Connection member private messaged another member, stating "I'm selling the license for a 100% private software (bank trojan). Expensive," and provided an email address. This message concerned the sale of malware to be used in unlawful computer intrusions.

13. It was further part of the conspiracy that BURKOV appointed a number of co-conspirators to leadership positions within Direct Connection in order to help him administer Direct Connection and further its criminal aims. In particular, BURKOV appointed approximately a dozen "Moderators," whose job it was to moderate the discussions on the particular forums to which they were assigned. BURKOV maintained at least two "Administrators," himself and a partner, who had authority over the forum as a whole. BURKOV also appointed a person to be in charge of escrow services to facilitate criminal deals among Direct Connection members and an "Arbiter" who adjudicated disputes between Direct Connection members, as further described in paragraph 15 below.

14. Direct Connection's membership included some of the world's most elite cybercriminals, including but not limited to the following:

a. Direct Connection member "Carlos," also known as "aqua," was one of the early members of the forum and moderated the banking sub-forum for many

years. Carlos used Direct Connection to advertise malware designed to steal banking information from victim computers. Carlos, whose real name is Maksim Yakubets, has been indicted in the Western District of Pennsylvania and the District of Nebraska for crimes arising from his use and distribution of malware. The State Department has offered a $5 million reward for information leading to his arrest or conviction.

b. Direct Connection member "Harderman," also known as "Gribodemon," joined the Direct Connection forum in 2010 and immediately began using the forum to promote his malware products, including ZeuS banking trojan version 2.0 and later the SpyEye banking trojan. In 2016, Harderman, whose real name is Aleksandr Andreevich Panin, was sentenced to nine years and six months in prison by the U.S. District Court for the Northern District of Georgia. BURKOV personally vouched for Harderman's admission to Direct Connection, stating in 2010: "His software is worthy of respect, in my opinion it has already surpassed the long famous Ze[uS] :-) I've known him about a year, about as long as I've used his product. I am as happy as a clam about our cooperation, he always helped, he never lets a question go unanswered, in general he has provided support above and beyond. I confirm fin. responsibility $2,000."

c. DirectConnection member "WebHost" offered a variety of criminal services to the Direct Connection members in a long-running Direct Connection thread titled "Hosting/Servers/Domains/VPS high-end quality." WebHost's real name is Mykhaylo Rytikov of Ukraine. Rytikov has been indicted in three separate federal districts in the United States, including the Eastern District of Virginia. The charges against Rytikov arise from, among other crimes, providing "bullet-proof hosting," i.e., secure servers designed to be outside of the reach of law enforcement and used in criminal schemes.

d. Direct Connection member "Centurion" was the moderator of the sub-forum for security and anonymity. This was one of several forums on which this person both occupied a position of authority and used that position to facilitate trafficking in stolen financial data. "Centurion," whose real name was Sergey Vovnenko, was arrested in June 2014 and extradited to the United States. In 2017, Vovenko was sentenced to 41 months in prison by the U.S. District Court for the District of New Jersey for operating a botnet, stealing login and payment card data, and related crimes.

15. It was further part of the conspiracy that, in order to build trust among Direct Connection's criminal members and to facilitate criminal partnerships among Direct Connection's members, BURKOV developed a formal dispute resolution mechanism that governed Direct Connection members. Direct Connection members who had disputes with other members regarding their unlawful criminal agreements could file "suits" against each other that would be adjudicated by Direct Connection's officers. Members who did not abide by the decisions of Direct Connection's officers in regards to these "suits" could be expelled from the forums. For example, on or about April 2, 2014, a member of Direct Connection filed the following "suit" against another, accusing the other member of failing to provide agreed-upon "logs," which refers to information stolen via computer hacking that may contain login credentials for email or banking accounts and financial information. Following the formality required by Direct Connection, the Direct Connection member posted the following to the forum:

> I, [redacted], am aware of the Forum's terms and conditions, am responsible for the accuracy of given facts and speculations, and am aware that as a result of this suit my opponent and I can lose our membership on the Forum. **Plaintiff:** [redacted]. **Defendant:** [redacted] **Case:** purchased accounts from logs, ignored in Jabber. **Cost:** 560 WMZ. **Description:** On March 14, 2014 I agreed to buy accounts from logs; this person answered that he would transfer the material the next day because at that moment he wasn't at his working computer. I agreed and transferred WMZ the same day. The next day I did not receive any accounts, nor did I receive them the day after. I was ignored; he answered me once in 3 days that he is busy etc. I was and am asking the defendant to send the money back as those logs are not important anymore, and we had agreed the time in the first place. I will send logs and contacts upon request.

16. It was further part of the conspiracy that Direct Connection members would post advice to the rest of the members to assist them in avoiding arrest. For instance, on or about April 11, 2014, a Direct Connection member posted a thread under the forum "News" regarding an article entitled, "Russian Ministry of Foreign Affairs: The growing threat of Russian citizens being

detained on the USA demand." In the same thread, the Direct Connection member posted the following: "Here's a list of countries that practice extradition, if anyone's interested: xttp://www.state.gov/documents/organization/71600.pdf."

17. It was further part of the conspiracy that BURKOV used Direct Connection both to advertise the unlawful services he offered, and to locate co-conspirators offering unlawful services BURKOV desired. These advertisements frequently resulted in BURKOV finding co-conspirators with whom he would conspire to commit the criminal aims of the conspiracy. In particular:

a. On or about November 2011, BURKOV made a posting on Direct Connection that advertised the Cardplanet Website with the title "Cardplanet.cc CVV2 & Dumps." The posting stated "We are proud to introduce you to the planet of card." The purpose and effect of this posting was to drive Direct Connection members to the Cardplanet Website so as to aid and facilitate the illegal aims of the website.

b. On or about January 20, 2011, BURKOV made a post to Direct Connection's membership discussing how he and his team use "SpyEye" which is operated by a Direct Connection member. SpyEye was a banking trojan, *i.e.*, malware designed to steal information like banking credentials and other financial information from infected computers. SpyEye was used to steal financial information from computers around the world, including computers in the United States. In his post, BURKOV stated "we" have been using SpyEye for two years and that is how he partially makes his living, and he and his accomplices were "happy as clams" with it. The administer of SpyEye, Aleksandr Andreevich Panin, was a member of Direct Connection. BURKOV and Panin discussed SpyEye via direct messages on Direct Connection. In particular, BURKOV asked Panin for assistance in operating SpyEye and informed Panin that SpyEye was a great project.

18. It was further part of the conspiracy that BURKOV actively managed Direct Connection. For instance,

a. On February 23, 2009, BURKOV made an early post under "Opening the Forum" to Direct Connection welcoming everyone to the forum and stating that members can post any requests or questions to "us" here.

b. On April 22, 2009, a Direct Connection member posted that the forum turned out very nice and congratulations were in order for BURKOV "&Co". In response, BURKOV said "thank you for the pleasant words and welcome."

c. On July 20, 2009, a Direct Connection member asked about the policies for selecting officer positions of moderators and arbiters of Direct Connection, and asked if it was just "who knows [BURKOV] best" or who is working with him? In response, BURKOV wrote they were all in charge and asked what officer selection policy the member thought would be best.

d. On March 23, 2011, a Direct Connection member asked BURKOV if he could remove his name as a moderator because he no longer served in that position. BURKOV responded that it had been done.

Conclusion

19. The Statement of Facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

20. The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident, or other innocent reason.

G. Zachary Terwilliger
United States Attorney

By: _____
Kellen S. Dwyer
Alexander P. Berrang
Assistant United States Attorneys

Laura Fong
Senior Trial Attorney
Computer Crime & Intellectual Property Section
U.S. Department of Justice

Defendant's Signature: After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 1/23/, 2020

Aleksei Yurievich Burkov
Defendant

Defense Counsel Signature: I am Aleksei Yurievich Burkov's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 1/23/20, 2020

Gregory Stambaugh, Esq.
Counsel for the Defendant